Kakde, M. and Wojtkowiak, Z.
Osaka J. Math.
58 (2021), 149–170

A NOTE ON THE MAIN CONJECTURE OVER $\mathbb{Q}$

Mahesh KAKDE and Zdzisław WOJTKOWIAK

(Received January 4, 2019, revised September 20, 2019)

Abstract

In this note we show how the main conjecture of the Iwasawa theory over $\mathbb{Q}$ has a natural place in the context of the Galois representation of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on the etale pro-p fundamental group of the projective line minus three points. However we still need to assume the Vandiver conjecture to get a proof of the main conjecture in this context.

1. Introduction

Let us fix an odd prime number p. We fix an embedding of an algebraic closure of $\mathbb{Q}$ into the complex numbers, i.e. the embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$ once for all. We denote by μ_{p^n} the subgroup of all p^n-th roots of 1. We denote by ξ_{p^n} a primitive p^n-th root of 1. We set $\mu_{p^\infty} := \bigcup_{n=1}^{\infty} \mu_{p^n}$. For n a natural number or ∞ we denote by $\mathbb{Q}(\mu_{p^n})^+$ the maximal subfield of $\mathbb{Q}(\mu_{p^n})$ contained in the field of real numbers $\mathbb{R}$.

Let $\mathcal{M}_p$ (resp. M_p) be the maximal abelian pro-p extension of $\mathbb{Q}(\mu_{p^\infty})$ (resp. $\mathbb{Q}(\mu_{p^\infty})^+$) unramified outside p. Let us denote

$$X_\infty = Gal(M_p/\mathbb{Q}(\mu_{p^\infty})^+)$$

and

$$G = Gal(\mathbb{Q}(\mu_{p^\infty})^+/\mathbb{Q}).$$

The group G acts on X_∞ by conjugation and hence X_∞ is a $\mathbb{Z}_p[[G]]$-module. By a well-known theorem of Iwasawa X_∞ is a finitely generated torsion $\mathbb{Z}_p[[G]]$-module. The structure theorem of finitely generated torsion $\mathbb{Z}_p[[G]]$-modules then implies that X_∞ is pseudo-isomorphic to $\oplus_i \mathbb{Z}_p[[G]]/(f_i)$ for some $f_i \in \mathbb{Z}_p[[G]]$. The main conjecture of Iwasawa theory, proved by Mazur-Wiles [11] and independently by Rubin (appendix in [10]), states that

$$(\prod f_i) = \zeta_{\mathbb{Q},p} \cdot I(\mathbb{Z}_p[[G]]),$$

where $I(\mathbb{Z}_p[[G]])$ is the augmentation ideal and $\zeta_{\mathbb{Q},p} \in Frac(\mathbb{Z}_p[[G]])$ is the p-adic zeta function of Kubota-Leopoldt. For a more detailed description the reader should consult [1, pages 1-8].

Let $\mathcal{L}_p$ be the maximal abelian pro-p extension of $\mathbb{Q}(\mu_{p^\infty})$ unramified everywhere. Then $\mathcal{L}_p$ is contained in $\mathcal{M}_p$. Let

$$\Gamma := Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times .$$

2010 Mathematics Subject Classification. Primary 11R23; Secondary 11R18, 11S40, 11R32.

The identification of $Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ with $\mathbb{Z}_p^\times$ is given by the cyclotomic character. In the paper we shall always denote by Γ the group $\mathbb{Z}_p^\times$ acting on various objects, while we shall keep the notation $\mathbb{Z}_p^\times$, when it is viewed as a subset of $\mathbb{Z}_p$.

The group Γ acts on $Gal(\mathcal{L}_p/\mathbb{Q}(\mu_{p^\infty}))$ by conjugation. The main conjecture can also be stated in terms of the $\mathbb{Z}_p[[\Gamma]]$-module $Gal(\mathcal{L}_p/\mathbb{Q}(\mu_{p^\infty}))$ (see [1, the beginning of Section 1.4] and [14, Chapter 15, Section 15.4]). In this note we present a proof of the main conjecture for $Gal(\mathcal{L}_p/\mathbb{Q}(\mu_{p^\infty}))$, assuming the Vandiver conjecture for a prime p. We remark that it was already observed by Iwasawa that the main conjecture is a consequence of Vandiver's conjecture. We place our proof in the context of the natural representation of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on the pro-p etale fundamental group of $\mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0, 1, \infty\}$ based at the tangential point $\overrightarrow{10}$, where the main conjecture over $\mathbb{Q}$ has perhaps its natural place. We point out that the p-adic zeta function of Kubota-Leopoldt appears naturally, while considering this Galois representation (see [17]).

Our proof is based on construction of the cocycle

$$\mathfrak{A}(\overrightarrow{10}) : G_{\mathbb{Q}} \to \mathbb{Z}_p[[\mathbb{Z}_p]]$$

defined in [17] (and denoted there by ζ_p), whose construction will be given in Section 2 and on the Ihara's formula

$$\int_{\mathbb{Z}_p^\times} x^{m-1} d\mathfrak{A}(\overrightarrow{10})([cl](\epsilon))(x) = L_p(m, \omega^{1-m})(1 - p^{m-1})CW_m(\epsilon),$$

for $m > 1$ and odd (see [7, formula on the page 105]).

Let us explain briefly the notations and objects appearing in the formula. Let $\mathcal{U}_\infty^1$ be the projective limit with respect to the relative norm maps of the principal units of $\mathbb{Q}_p(\mu_{p^n})$. Let $\mathcal{K}_p$ be the field extension of $\mathbb{Q}(\mu_{p^\infty})$ generated by all p powers roots of $1 - \xi_{p^n}^i$ for all n and all $0 < i < p^n$. In the formula, $\epsilon \in \mathcal{U}_\infty^1$, $[cl] : \mathcal{U}_\infty^1 \to Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty})$ is induced from the local class field theory maps, $CW_n : \mathcal{U}_\infty^1 \to \mathbb{Z}_p$ are Coates-Wiles homomorphisms, L_p is the p-adic L-function of Kubota-Leopoldt and ω is the Teichmüller character. Our principal result is the following consequence of the Ihara's formula.

Proposition 1.1. *Let $\epsilon \in \mathcal{U}_\infty^1$. Then*

$$\mathfrak{A}(\overrightarrow{10})^\times([cl](\epsilon)) = \zeta_p \cdot \mu^\times_{\Delta(f_\epsilon)}$$

as pseudo-measures on $\mathbb{Z}_p^\times$. (Using the well-known isomorphism between the ring of measures on $\mathbb{Z}_p^\times$ and the ring $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ we may consider the above equation as an equality in the total ring of fractions of $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$).

In the last formula, f_ϵ is the Coleman power series associated to ϵ, the power series $\Delta(f_\epsilon)$ is defined by $(\Delta(f_\epsilon))(T) = (1 + T)f'_\epsilon(T)/f_\epsilon(T)$. Further, μ_g denotes the measure on $\mathbb{Z}_p$ associated to a power series $g(T) \in \mathbb{Z}_p[[T]]$ (again we have implicitly used isomorphisms between the ring of $\mathbb{Z}_p$-values measures on $\mathbb{Z}_p$, the ring $\mathbb{Z}_p[[\mathbb{Z}_p]]$ and the ring $\mathbb{Z}_p[[T]]$, the latter obtained by fixing $1 \in \mathbb{Z}_p$ as its topological generator) and $\mu^\times$ denotes the restriction of a measure μ on $\mathbb{Z}_p$ to $\mathbb{Z}_p^\times$. The element ζ_p is the p-adic zeta function we shall construct in this paper.

Corollary 1.2. *Let*

$$\mathfrak{A}(\overrightarrow{10})^{\times} : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty})) \to \mathbb{Z}_p[[\mathbb{Z}_p^{\times}]]$$

be induced by $\mathfrak{A}(\overrightarrow{10}) : G_{\mathbb{Q}} \to \mathbb{Z}_p[[\mathbb{Z}_p]]$ *by restriction of a measure on* $\mathbb{Z}_p$ *to* $\mathbb{Z}_p^{\times}$. *Then we have an isomorphism of* $\mathbb{Z}_p[[\Gamma]]$*-modules*

$$Gal(\mathcal{K}_p/\mathcal{K}_p \cap \mathcal{L}_p) \cong (\zeta_p)$$

where (ζ_p) *is the augmentation ideal of* $\mathbb{Z}_p[[\mathbb{Z}_p^{\times}]]$ *times* ζ_p.

The action of $\mathbb{Z}_p[[\Gamma]]$ on $\mathbb{Z}_p[[\mathbb{Z}_p^{\times}]]$ will be defined in Section 2. In particular the action of $-1 \in \Gamma$ is an involution, hence any $\mathbb{Z}_p[[\Gamma]]$-module is a direct sum of the + and − parts.

Lemma 1.3. *Let us assume the Vandiver conjecture. Then the map*

$$\mathfrak{A}(\overrightarrow{10})^{\times} : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty})) \to \mathbb{Z}_p[[\mathbb{Z}_p^{\times}]]^{-}$$

is an isomorphism.

This consequence of the Vandiver conjecture is in fact well known (see [7, Section II, Theorem 6], [2, Theorem (7.33)], [5, Theorem C] and [6, corollary on page 62]). The proofs there use the Ihara power series from [7]. The proof presented in this note is simpler, and moreover it can be applied in more situations, for example to study surjectivity of Soulé classes for roots of unity or more generally of l-adic Galois polylogarithms introduced in [15], though in fact it has some common points with the alternative proof given on page 333 in [5]. The proof of the main conjecture over $\mathbb{Q}$ is then an easy consequence of Corollary 1.2 and Lemma 1.3. Our last result is the generalization of the Ihara's formula for all integers m. The case $m = 1$ is the most interesting as then the residue at 1 of the p-adic zeta function appears.

2. The cocycle associated to the path from $\overrightarrow{01}$ to $\overrightarrow{10}$

Recall that we have fixed an embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$. Let $V_n = \mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus (\{0, \infty\} \cup \mu_{p^n})$ and let γ_n be a path on V_n from $\overrightarrow{01}$ to $\frac{1}{p^n}\overrightarrow{10}$ along the interval $[0, 1]$. Let $\pi_1(V_n, \overrightarrow{01})$ denote the etale pro-p fundamental group of V_n based at $\overrightarrow{01}$. We denote by x_n and by $y_{k,n}$ for $0 \leqslant k < p^n$ the standard topological generators of $\pi_1(V_n, \overrightarrow{01})$, loops around 0 and $\xi_{p^n}^k$ for $0 \leqslant k < p^n$ respectively (see [16, Section 1]).

Let $\sigma \in G_{\mathbb{Q}}$. Then, written additively,

$$\gamma_n^{-1}\sigma(\gamma_n) \equiv \sum_{i=0}^{p^n-1} \alpha_i^{(n)}(\sigma) y_{i,n} \text{ modulo } (\pi_1(V_n, \overrightarrow{01}), \pi_1(V_n, \overrightarrow{01})),$$

for some coefficients $\alpha_i^{(n)}(\sigma) \in \mathbb{Z}_p$.

Proposition 2.1 (see [13], [16] and [17])**.** *For any* $\sigma \in G_{\mathbb{Q}}$ *the family of functions*

$$\{\mathfrak{A}^{(n)}(\overrightarrow{10})(\sigma) : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p, i \mapsto \alpha_i^{(n)}(\sigma)\}_{n \in \mathbb{N}}$$

defines a measure, denoted $\mathfrak{A}(\overrightarrow{10})(\sigma)$*, on* $\mathbb{Z}_p$ *with values in* $\mathbb{Z}_p$.

It follows from the proposition that we get a continuous function

$$\mathfrak{A}(\overrightarrow{10}) : G_{\mathbb{Q}} \to \mathbb{Z}_p[[\mathbb{Z}_p]].$$

Let $\tau, \sigma \in G_{\mathbb{Q}}$. It follows from the identity $\gamma_n^{-1}((\tau\sigma)(\gamma_n)) = (\gamma_n^{-1}\tau(\gamma_n)) \cdot \tau(\gamma_n^{-1}\sigma(\gamma_n))$ that

$$\alpha_i^{(n)}(\tau\sigma) = \alpha_i^{(n)}(\tau) + \chi(\tau)\alpha^{(n)}_{\chi^{-1}(\tau)i}(\sigma). \tag{1}$$

From the last two identities we get

$$\alpha_i^{(n)}(\tau\sigma\tau^{-1}) = \alpha_i^{(n)}(\tau) - \chi(\sigma)\alpha^{(n)}_{\chi^{-1}(\sigma)i}(\tau) + \chi(\tau)\alpha^{(n)}_{\chi^{-1}(\tau)i}(\sigma). \tag{2}$$

This identity (2) motivates the next definition.

DEFINITION 2.2. We define the action of $\Gamma = \mathbb{Z}_p^\times$, hence the action of $G_{\mathbb{Q}}$ via the p-cyclotomic character, on $\mathbb{Z}_p[[\mathbb{Z}_p]]$ by the formula

$$c(\sum_{i=1}^{m} a_i[x_i]) := \sum_{i=1}^{m} ca_i[cx_i] \tag{3}$$

for elements of $\mathbb{Z}_p[\mathbb{Z}_p]$ and we extend by continuity to the action on $\mathbb{Z}_p[[\mathbb{Z}_p]]$.

It follows immediately from the identity (1) that the function

$$\mathfrak{A}(\overrightarrow{10}) : G_{\mathbb{Q}} \to \mathbb{Z}_p[[\mathbb{Z}_p]]$$

is a cocycle.

Let a belong to a number field K contained in $\overline{\mathbb{Q}}$. We denote by

$$\kappa(a) : G_{K(\mu_{p^\infty})} \to \mathbb{Z}_p$$

the Kummer character associated to a.

Proposition 2.3 (see Proposition 2 in [17][1])**.** *Let $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$. Then*

$$\mathfrak{A}^{(n)}(\overrightarrow{10})(\sigma) = \kappa(\frac{1}{p^n})(\sigma)[0] + \sum_{i=1}^{p^n-1} \kappa(1-\xi_{p^n}^i)(\sigma)[i].$$

We recall from the introduction that

$$\mathcal{K}_p := \mathbb{Q}_p(\mu_{p^\infty})((1-\xi_{p^n}^i)^{1/p^m} : 0 < i < p^n, n, m \in \mathbb{N}).$$

Observe that $\mathcal{K}_p$ is an abelian, unramified outside p, pro-p extension of $\mathbb{Q}(\mu_{p^\infty})$. Let $\tau \in Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ and $\overline{\tau}$ be a lifting of τ to $Gal(\mathcal{K}_p/\mathbb{Q})$. The group $\Gamma = Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times$ acts on $Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))$ by the standard formula

$$\tau(\sigma) = \overline{\tau}\sigma\overline{\tau}^{-1}.$$

It follows from Proposition 2.3 that the map $\mathfrak{A}(\overrightarrow{10}) : G_{\mathbb{Q}} \to \mathbb{Z}_p[[\mathbb{Z}_p]]$ factors through the Galois group $Gal(\mathcal{K}_p/\mathbb{Q})$. We denote the restriction of $\mathfrak{A}(\overrightarrow{10}) : Gal(\mathcal{K}_p/\mathbb{Q}) \to \mathbb{Z}_p[[\mathbb{Z}_p]]$ to the subgroup $Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))$ also by $\mathfrak{A}(\overrightarrow{10})$.

[1]We thank Guido Kings for kindly informing us that this cocycle is explained in much greater generality in his paper [9] as the etale realisation of the polylogarithm for commutative group scheme, with our case being that of $\mathbb{G}_m$.

Proposition 2.4. *The map*

$$\mathfrak{A}(\overrightarrow{10}) : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty})) \to \mathbb{Z}_p[[\mathbb{Z}_p]]$$

is a continuous injective homomorphism of $\mathbb{Z}_p[[\Gamma]]$*-modules.*

Proof. The formula (1) implies that $\mathfrak{A}(\overrightarrow{10})$ is a morphism of $\mathbb{Z}_p$ modules. It follows from equation (2) that that for $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$ we have

$$\alpha_i^{(n)}(\tau\sigma\tau^{-1}) = \chi_{(\tau)}\alpha^{(n)}_{\chi^{-1}(\tau)i}(\sigma)$$

Therefore

$$\sum_{i=0}^{p^n-1} \alpha_i^{(n)}(\tau\sigma\tau^{-1})[i] = \sum_{i=0}^{p^n-1} \chi(\tau)\alpha^{(n)}_{\chi(\tau)^{-1}i}(\sigma)[i] = \chi(\tau)\sum_{j=0}^{p^n-1} \alpha_j^{(n)}(\sigma)[\chi(\tau)j].$$

Hence it follows that $\mathfrak{A}(\overrightarrow{10})$ is a Γ-map. The injectivity follows from the definition of the field $\mathcal{K}_p$ and the explicit description of $\mathfrak{A}(\overrightarrow{10})$ given in Proposition 2.3. □

3. The restriction to $\mathbb{Z}_p^\times$

The multiplicative group $\mathbb{Z}_p^\times$ is a closed and open subset of $\mathbb{Z}_p$. It follows from the formula in equation (3) that the restriction map

$$\mathcal{R} : \mathbb{Z}_p[[\mathbb{Z}_p]] \to \mathbb{Z}_p[[\mathbb{Z}_p^\times]],$$

which associates to a measure μ on $\mathbb{Z}_p$ its restriction to $\mathbb{Z}_p^\times$, is a morphism of $\mathbb{Z}_p[[\Gamma]]$-modules. We shall also denote the measure $\mathcal{R}(\mu)$ by $\mu^\times$. For $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{p^\infty}))$, we denote the restriction of the measure $\mathfrak{A}(\overrightarrow{10})(\sigma)$ to $\mathbb{Z}_p^\times$, by $\mathfrak{A}(\overrightarrow{10})^\times(\sigma)$. We denote the composition

$$z_p : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty})) \xrightarrow{\mathfrak{A}(\overrightarrow{10})} \mathbb{Z}_p[[\mathbb{Z}_p]] \xrightarrow{\mathcal{R}} \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$$

by z_p. The action of $-1 \in \Gamma$ is an involution, hence $Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))$ and $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ are the direct sums of their + and − parts. Moreover, z_p induces a morphism of $\mathbb{Z}_p[[\Gamma]]$-modules

$$z_p^\epsilon : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))^\epsilon \to \mathbb{Z}_p[[\mathbb{Z}_p^\times]]^\epsilon,$$

for $\epsilon \in \{+, -\}$.

Proposition 3.1 (See also [17], Corollary 1)**.** *We have*

(i) *The morphisms z_p and z_p^- are injective.*
(ii) *The group $Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))^+ = 0$.*

Proof. Observe that $\kappa(1 - \xi_{p^n}^i)$, for $0 < i < p^n$ and $(i, p) > 1$, as well as $\kappa(\frac{1}{p^n})$ can be expressed as sums of $\kappa(1 - \xi_{p^n}^k)$ with $0 < k < p^n$ and $(k, p) = 1$. Hence it follows from Propositions 2.3 and 2.4 that z_p is injective.

Let $a = (\sum_{i=0}^{p^n-1} a_i^{(n)}[i])_{n\in\mathbb{N}} \in \mathbb{Z}_p[[\mathbb{Z}_p]]$. Then $(-1) \in \Gamma$ acts on a as follows

$$(-1)a = \left(-a_0^{(n)}[0] - \sum_{i=1}^{p^n-1} a_i^{[n]}[p^n - i]\right)_{n\in\mathbb{N}}.$$

Hence it follows that

$$a^+ = \frac{1}{2}\left(\sum_{i=1}^{p^n-1}(a_i^{(n)} - a_{p^n-i}^{(n)})[i]\right)_{n\in\mathbb{N}} \tag{4}$$

and

$$a^- = \frac{1}{2}\left(2a_0^{(n)}[0] + \sum_{i=1}^{p^n-1}(a_i^{(n)} + a_{p^n-i}^{(n)})[i]\right)_{n\in\mathbb{N}}. \tag{5}$$

For $\sigma \in Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))$, we have

$$\mathfrak{U}(\overrightarrow{10})(\sigma) = \left(\kappa\left(\frac{1}{p^n}\right)(\sigma)[0] + \sum_{i=1}^{p^n-1}\kappa(1-\xi_{p^n}^{-i})(\sigma)[i])\right)_{n\in\mathbb{N}}$$

by Proposition 2.3. The identity $1-\xi_{p^n}^{-i} = (-\xi_{p^n}^{-i})(1-\xi_{p^n}^{i})$ implies that $\kappa(1-\xi_{p^n}^{-i}) = \kappa(1-\xi_{p^n}^{i})$ on $Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))$. Hence it follows that for $\sigma \in Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))$, we have $\mathfrak{U}(\overrightarrow{10})(\sigma)^+ = 0$ and

$$\mathfrak{U}(\overrightarrow{10})(\sigma)^- = \left(\kappa(\frac{1}{p^n})(\sigma)[0] + \sum_{i=1}^{p^n-1}\kappa(1-\xi_{p^n}^{i})(\sigma)[i]\right)_{n\in\mathbb{N}}.$$

Therefore

$$Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))^+ = 0$$

and the map z_p^- given by

$$z_p^-(\sigma) = \left(\sum_{i=1,(i,p)=1}^{p^n-1}\kappa(1-\xi_{p^n}^{i})(\sigma)[i]\right)_{n\in\mathbb{N}}$$

is injective. □

Let $\mathcal{E}_n$ be the group of p-units in $\mathbb{Q}(\mu_{p^n})$, i.e. $\mathcal{E}_n = \mathbb{Z}[\mu_{p^n}]\left[\frac{1}{p}\right]^\times$ and let $\mathcal{C}_n$ be the group of cyclotomic p-units of $\mathbb{Q}(\mu_{p^n})$, i.e. the subgroup of $\mathcal{E}_n$ generated by μ_{p^n} and elements $1-\xi_{p^n}^k$ for $0 < k < p^n$. Let S_n be a set of all integers between 0 and $p^n/2$ that are coprime to p.

Lemma 3.2. *The following conditions are equivalent:*

(i) *the map*

$$\alpha_n : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^n})) \to \oplus_{i\in S_n}\mathbb{Z}/p^n\mathbb{Z}$$

given by

$$\sigma \mapsto (\kappa(1-\xi_{p^n}^{i})(\sigma))_{i\in S_n},$$

is surjective;

(ii) *p does not divide $|\mathcal{E}_n/\mathcal{C}_n|$.*

Proof. The map

$$\mathcal{E}_n/\mathcal{E}_n^{p^n} \to \mathbb{Q}(\mu_{p^n})^\times/\mathbb{Q}(\mu_{p^n})^{\times p^n}$$

induced by the inclusion $\mathcal{E}_n \subset \mathbb{Q}(\mu_{p^n})^\times$ is injective. Therefore by the Kummer theory the map α_n is surjective if and only if the subgroup of $\mathcal{E}_n/\mathcal{E}_n^{p^n}$ generated by elements $1-\xi_{p^n}^i$, $i \in S_n$ is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^{|S_n|}$. It follows from [14, Theorem 8.9] that there is no multiplicative relation between ξ_{p^n} and the elements $1-\xi_{p^n}^i$ for $i \in S_n$. Hence α_n is surjective if and only if the subgroup of $\mathcal{E}_n/\mathcal{E}_n^{p^n}$ generated by elements $1-\xi_{p^n}^i$, $i \in S_n$ and by ξ_{p^n} is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^{|S_n|+1}$. The last condition holds if and only if the subgroup of $\mathcal{E}_n/\mathcal{E}_n^p$ generated by elements $1-\xi_{p^n}^i$, $i \in S_n$ and by ξ_{p^n} is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{|S_n|+1}$.

If p divides $|\mathcal{E}_n/\mathcal{C}_n|$ then there is $u \in \mathcal{E}_n$ such that $u^p \in \mathcal{C}_n$ but $u \notin \mathcal{C}_n$. Any element of $\mathcal{C}_n$ can be written in a unique way in the form $\pm\xi_{p^n}^{a_0}\prod_{i\in S_n}(1-\xi_{p^n}^i)^{a_i}$ (see [14, Theorem 8.9]). Hence

$$u^p = \pm\xi_{p^n}^{a_0}\prod_{i\in S_n}(1-\xi_{p^n}^i)^{a_i},$$

where at least one of $a_i \not\equiv 0$ modulo p. But then the subgroup of $\mathcal{E}_n/\mathcal{E}_n^p$ generated by ξ_{p^n} and $1-\xi_{p^n}^i$ for $i \in S_n$ will have the rank smaller than $|S_n|+1$. Therefore i) implies ii).

If p does not divide $|\mathcal{E}_n/\mathcal{C}_n|$ then the map $\mathcal{C}_n/\mathcal{C}_n^p \to \mathcal{E}_n/\mathcal{E}_n^p$ is injective. The elements ξ_{p^n} and $1-\xi_{p^n}^i$ for $i \in S_n$ taken modulo $\mathcal{C}_n^p$ form a basis of $\mathcal{C}_n/\mathcal{C}_n^p$. But it implies, going backwards all equivalent statements, that i) holds. □

Lemma 3.3. *The following conditions are equivalent:*

(i) *the map*

$$z_p^- : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty})) = Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))^- \to \mathbb{Z}_p[[\mathbb{Z}_p^\times]]^-$$

is an isomorphism of $\mathbb{Z}_p[[\Gamma]]$-modules;

(ii) *p does not divide $|\mathcal{E}_n/\mathcal{C}_n|$ for all $n \geqslant 1$.*

Proof. If p does not divide $|\mathcal{E}_n/\mathcal{C}_n|$ then the map

$$\alpha_n : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^n})) \to \oplus_{i\in S_n}\mathbb{Z}/p^n\mathbb{Z}$$

given by

$$\sigma \mapsto (\kappa(1-\xi_{p^n}^i)(\sigma))_{i\in S_n},$$

is surjective by Lemma 3.2. Let $m \geqslant n$. Let us assume that p does not divide $|\mathcal{E}_m/\mathcal{C}_m|$. Then it follows from a theorem of Bass (see [14, page 150 and Theorem 8.9]) that the map

$$\alpha_n^{(m)} : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^m})) \to \oplus_{i\in S_n}\mathbb{Z}/p^m\mathbb{Z}$$

given by

$$\sigma \mapsto (\kappa(1-\xi_{p^n}^i)(\sigma))_{i\in S_n},$$

is surjective. Hence the assumption ii) implies that for all $n \in \mathbb{N}$ the maps

$$\alpha_n^\infty : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty})) \to \oplus_{i\in S_n}\mathbb{Z}_p$$

given by

$$\sigma \mapsto (\kappa(1-\xi_{p^n}^i)(\sigma))_{i\in S_n},$$

are surjective. Therefore the map

$$z_p^- : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty})) \to \mathbb{Z}_p[[\mathbb{Z}_p^\times]]^-$$

is surjective. Hence it follows from Proposition 3.1 that the map z_p^- is an isomorphism.

It follows from Lemma 3.2 that i) implies ii). □

4. The multiplicative structure of $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$

We denote by $\mathbb{Z}_p(k)$ the ring $\mathbb{Z}_p$ equipped with the action of Γ given by

$$x(a) := x^k a.$$

The infinite product $\prod_{k=1}^\infty \mathbb{Z}_p(k)$ is equipped with a multiplicative structure given by

$$(a_k)_{k=1}^\infty \cdot (b_k)_{k=1}^\infty = (a_k b_k)_{k=1}^\infty.$$

The $\mathbb{Z}_p[[\Gamma]]$-module $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ has a multiplication induced by a group multiplication in $\mathbb{Z}_p^\times$. Let us define a map

$$\Phi : \mathbb{Z}_p[[\mathbb{Z}_p^\times]] \to \prod_{k=1}^\infty \mathbb{Z}_p(k)$$

by the formula

$$\Phi(\mu) = \left(\int_{\mathbb{Z}_p^\times} x^{k-1} d\mu(x) \right)_k.$$

Lemma 4.1. *The map Φ is a continuous injective morphism of $\mathbb{Z}_p[[\Gamma]]$-modules. Moreover, $\Phi(\mu \cdot \nu) = \Phi(\mu)\Phi(\nu)$ for any $\mu, \nu \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$.*

Proof. It is evident that Φ is continuous. Let us first show that the map Φ is a map of $\mathbb{Z}_p[[\Gamma]]$-modules. By continuity of Φ it is enough to check that $\Phi(g\mu) = g\Phi(\mu)$ for each $g \in \Gamma$ and for $\mu = \sum_{x \in \mathbb{Z}_p^\times} a_x[x] \in \mathbb{Z}_p[\mathbb{Z}_p^\times]$. By our convention (see formula (3))

$$g\mu = \sum_x g a_x [gx].$$

Hence

$$\Phi(g\mu) = \left(\sum_x g^k x^{k-1} a_x \right)_k = g \cdot \left(\sum_x x^{k-1} a_x \right)_k = g\Phi(\mu).$$

Next we show that Φ is multiplicative i.e. $\Phi(\mu\nu) = \Phi(\mu)\Phi(\nu)$. Again by continuity we can need to check this for $\mu = \sum_x a_x[x]$ and $\nu = \sum_x b_x[x]$ in $\mathbb{Z}_p[\mathbb{Z}_p^\times]$. We have

$$\begin{aligned}
\Phi(\mu)\Phi(\nu) &= \left(\sum_x a_x x^{k-1} \right)_k \left(\sum_y b_y y^{k-1} \right)_k \\
&= \left(\sum_z \left(\sum_{x,y:xy=z} a_x b_y \right) z^{k-1} \right)_k \\
&= \Phi(\mu\nu).
\end{aligned}$$

□

Observe that

$$\left(\prod_{k=1}^{\infty}\mathbb{Z}_p(k)\right)^{+} = \prod_{k=1}^{\infty}\mathbb{Z}_p(2k)$$

and

$$\left(\prod_{k=1}^{\infty}\mathbb{Z}_p(k)\right)^{-} = \prod_{k=1}^{\infty}\mathbb{Z}_p(2k-1).$$

It follows from Proposition 3.1 and Lemma 4.1 that the composition

$$Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))^{-} \xrightarrow{z_p^{-}} \mathbb{Z}_p[[\mathbb{Z}_p^{\times}]]^{-} \xrightarrow{\Phi^{-}} \prod_{k=1}^{\infty}\mathbb{Z}_p(2k-1)$$

is an injective morphism of $\mathbb{Z}_p[[\Gamma]]$-modules.

5. The Coates-Wiles homomorphism

We recall briefly some results of Coleman presented in [1]. Let $\mathcal{U}_n := \mathbb{Z}_p[\mu_{p^{n+1}}]^{\times}$ and put $\mathcal{U}_\infty := \varprojlim_n \mathcal{U}_n$, with the projective limit taken with respect to the norm maps. Let $\mathcal{N} : \mathbb{Z}_p[[T]] \to \mathbb{Z}_p[[T]]$ be the norm map defined in [1]. Put $W := \{f \in \mathbb{Z}_p[[T]]^{\times} : \mathcal{N}(f) = f\}$. For each integer $n \geqslant 0$, we fix a primitive p^{n+1}-th root $\xi_{p^{n+1}}$ of 1 such that $\xi_{p^{n+1}}^{p} = \xi_{p^n}$.

We have

$$Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = Gal(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)\,.$$

Hence the group Γ acts on $\mathcal{U}_\infty$. It acts also on W by

$$(cf)(T) := f((1+T)^c - 1)$$

for $c \in \Gamma$ and $f(T) \in W$ (see [1, the formula (2.7)]).

Theorem 5.1 (See [1], Theorem 2.1.2 and Corollary 2.3.7)**.** *Let $\epsilon = (\epsilon_n) \in \mathcal{U}_\infty$, then there exists a unique $f_\epsilon(T) \in \mathbb{Z}_p[[T]]^{\times}$ such that $f(\xi_{p^{n+1}} - 1) = \epsilon_n$ for all $n \geqslant 0$. Moreover, the map $\epsilon \mapsto f_\epsilon(T)$ defines a Γ-isomorphism from $\mathcal{U}_\infty$ to W.*

Let us define $\Delta : \mathbb{Z}_p[[T]]^{\times} \to \mathbb{Z}_p[[T]]$ by

$$\Delta(f) := (1+T)f'(T)/f(T).$$

For $f \in \mathbb{Z}_p[[T]]$ we define

$$\varphi(f)(T) := f((1+T)^p - 1).$$

The trace operator $\psi : \mathbb{Z}_p[[T]] \to \mathbb{Z}_p[[T]]$ is a continuous $\mathbb{Z}_p$-homomorphism characterized by the identity

$$(\varphi \circ \psi)(f)(T) = \frac{1}{p}\sum_{\xi \in \mu_{p-1}} f(\xi(1+T) - 1).$$

We set

$$\mathbb{Z}_p[[T]]^{\psi = id} = \{f \in \mathbb{Z}_p[[T]] : \psi(f) = f\}.$$

We define a map

$$[Col] : \mathcal{U}_\infty \to \mathbb{Z}_p[[T]]$$

to be the map $\epsilon \mapsto \Delta(f_\epsilon(T))$. We define an action of Γ on $\mathbb{Z}_p[[T]]^{\psi=id}$ by

$$(cf)(T) := cf((1+T)^c - 1)$$

for $c \in \Gamma$ and $f(T) \in \mathbb{Z}_p[[T]]^{\psi=id}$.

Corollary 5.2. *The map* $[Col]$ *induces a surjective* Γ*-morphism*

$$[Col] : \mathcal{U}_\infty \to \mathbb{Z}_p[[T]]^{\psi=id}$$

with $ker([Col]) = \mu_{p-1}$.

Proof. It follows from Theorem 5.1 and from [1, Theorem 2.4.6 and Lemma 2.4.5] that $[Col]$ is surjective with $ker([Col]) = \mu_{p-1}$. One checks that the map from W to $\mathbb{Z}_p[[T]]^{\psi=id}$ given by $f \mapsto \Delta(f)$ is a Γ-morphism. Hence the map $[Col]$ is a Γ-morphism. □

We recall the definition of the Coates-Wiles homomorphisms. Let $\epsilon \in \mathcal{U}$. We define numbers CW_k^ϵ for $k \geqslant 1$ by the identity.

$$\Delta(f_\epsilon)(e^X - 1) = \sum_{k=1}^{\infty} \frac{CW_k^\epsilon}{(k-1)!} X^{k-1}. \tag{6}$$

We get then maps

$$CW_k : \mathcal{U}_\infty \to \mathbb{Z}_p(k).$$

which are Γ-morphisms (see [1, Lemma 2.6.2]). We recall that

$$\mathcal{P} : \mathbb{Z}_p[[\mathbb{Z}_p]] \to \mathbb{Z}_p[[T]]$$

is the Iwasawa isomorphism characterized by $\mathcal{P}([1]) = (1+T)$ and that in our notation if $f \in \mathbb{Z}_p[[T]]$ then $\mu_f := \mathcal{P}^{-1}(f)$. Then we have

$$f(e^X - 1) = \sum_{k=0}^{\infty} \Big(\int_{\mathbb{Z}_p} x^k d\mu_f(x) \Big) \frac{X^k}{k!}. \tag{7}$$

Lemma 5.3. *Let* $f \in \mathbb{Z}_p[[T]]^{\psi=id}$. *Then*

(i) $\mathcal{P}(\mu_f^\times) = f(T) - f((1+T)^p - 1)$,

(ii) $(1-p^k) \int_{\mathbb{Z}_p} x^k d\mu_f(x) = \int_{\mathbb{Z}_p^\times} x^k d\mu_f^\times(x)$.

Proof. Let $f \in \mathbb{Z}_p[[T]]^{\psi=id}$. The condition $\psi(f) = f$ is equivalent to the condition $(\varphi \circ \psi)(f) = \varphi(f)$. Hence it is equivalent to the equality

$$\frac{1}{p} \sum_{\xi \in \mu_p} f(\xi(1+T) - 1) = f((1+T)^p - 1). \tag{8}$$

The power series

$$\mathcal{P}(\mu_f^\times)(T) = f(T) - \frac{1}{p} \sum_{\xi \in \mu_p} f(\xi(1+T) - 1).$$

Hence if $f \in \mathbb{Z}_p[[T]]^{\psi=id}$ then

$$\mathcal{P}(\mu_f^{\times})(T) = f(T) - f((1+T)^p - 1).$$

Hence it follows that

$$f(e^X - 1) - f(e^{pX} - 1) = \sum_{k=0}^{\infty} \int_{\mathbb{Z}_p^{\times}} x^k d\mu_f^{\times}(x) \frac{X^k}{k!}.$$

On the other side we have that

$$f(e^X - 1) - f(e^{pX} - 1) = \sum_{k=0}^{\infty} \int_{\mathbb{Z}_p} x^k d\mu_f(x) \frac{X^k}{k!} - \sum_{k=0}^{\infty} \int_{\mathbb{Z}_p} x^k d\mu_f(x) \frac{p^k X^k}{k!}.$$

Hence it follows that

$$\int_{\mathbb{Z}_p^{\times}} x^k d\mu_f^{\times}(x) = (1 - p^k) \int_{\mathbb{Z}_p} x^k d\mu_f(x)$$

for $k \geqslant 0$. In particular, $\int_{\mathbb{Z}_p^{\times}} d\mu_f^{\times}(x) = 0$. □

We state the last result as a corollary.

Corollary 5.4. *Let $f \in \mathbb{Z}_p[[T]]^{\psi=id}$. Then*

$$\int_{\mathbb{Z}_p^{\times}} d\mu_f^{\times}(x) = 0.$$

Corollary 5.5. *Let $\epsilon \in \mathcal{U}_{\infty}$. Then*

$$(1 - p^k) CW_{k+1}^{\epsilon} = (1 - p^k) \int_{\mathbb{Z}_p} x^k d\mu_{\Delta(f_\epsilon)}(x) = \int_{\mathbb{Z}_p^{\times}} x^k d\mu_{\Delta(f_\epsilon)}^{\times}(x)$$

for $k \geqslant 0$.

Proof. Comparing the formulas (6) and (7) we get that $CW_{k+1}^{\epsilon} = \int_{\mathbb{Z}_p} x^k d\mu_{\Delta(f_\epsilon)}(x)$ for $k \geqslant 0$. Then the formulas of the corollary follow from the point (ii) of Lemma 5.3. □

6. Group of units

Following Ihara (see [7, Section IV, page 93]) we set

$$\mathcal{U}_n^1 := \{u \in \mathbb{Z}_p[\mu_{p^{n+1}}]^{\times} : N(u) = 1 \text{ and } u \equiv 1 (mod\ (\xi_{p^{n+1}} - 1))\},$$

where $N : \mathbb{Q}_p(\mu_{p^{n+1}}) \to \mathbb{Q}_p$ is the norm map. Let

$$\mathcal{U}_{\infty}^1 := \varprojlim_n \mathcal{U}_n^1$$

be the projective limit with respect to the relative norm maps.

Lemma 6.1. *We have $\mathcal{U}_{\infty}/\mathcal{U}_{\infty}^1 \cong (\mathbb{Z}/p)^{\times}$.*

Proof. Let

$$\mathcal{U}_n' = \{u \in \mathbb{Z}_p[\mu_{p^{n+1}}]^{\times} : u \equiv 1 (\mathrm{mod}\ (1 - \xi_{p^{n+1}}))\}$$

and $\mathcal{U}'_\infty = \varprojlim_n \mathcal{U}'_n$. We have $\mathcal{U}_n \cong \mathcal{U}'_n \times (\mathbb{Z}/p\mathbb{Z})^\times$ for all $n \geqslant 1$. Hence it follows that

$$\mathcal{U}_\infty \cong \mathcal{U}'_\infty \times (\mathbb{Z}/p\mathbb{Z})^\times.$$

Next we show that $\mathcal{U}'_\infty = \mathcal{U}^1_\infty$. Let $u_n \in \mathcal{U}'_n$. Then $N(u_n) \equiv 1 (\mathrm{mod}\ p^n)$ (see [4, page 113, exercise 4.a]). Let $(u_n) \in \varprojlim_n \mathcal{U}'_n$. Then for all $m \geqslant n$, we have $N(u_m) = N(N_{m,n}(u_m)) = N(u_n)$, where $N_{m,n}$ is the relative norm map. Hence $N(u_n) \equiv 1 (\mathrm{mod}\ p^m)$ for all $m \geqslant n$. Therefore $u_n \in \mathcal{U}^1_n$. Hence $\mathcal{U}'_\infty = \mathcal{U}^1_\infty$ and the result follows. □

Notice that $\mathcal{U}_\infty$ is not a $\mathbb{Z}_p[[\Gamma]]$-module. We define a structure of a $\mathbb{Z}_p[[\Gamma]]$-module on $\mathcal{U}^1_\infty$ in the following way. Let $\sum_{i=1}^k a_i\sigma_i \in \mathbb{Z}_p[Gal(\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q})]$ and $u \in \mathcal{U}^1_n$. Then we set

$$(\sum_{i=1}^k a_i\sigma_i)(u) := \prod_{i=1}^k (\sigma_i(u))^{a_i},$$

where $(\sigma_i(u))^{a_i} = 1 + \sum_{j=1}^\infty \binom{a_i}{j}(\sigma_i(u) - 1)^j$. It follows from Lemma 6.1 and from Theorem 5.1 and Corollary 5.2 that the map

$$[Col] : \mathcal{U}^1_\infty \to \mathbb{Z}_p[[T]]^{\psi=id}$$

is an isomorphism of $\mathbb{Z}[\Gamma]$-modules. Using the isomorphism $[Col]$ we define on $\mathbb{Z}_p[[T]]^{\psi=id}$ a structure of a $\mathbb{Z}_p[[\Gamma]]$-module, which is compatible with already given $\mathbb{Z}[\Gamma]$-module structure on $\mathbb{Z}_p[[T]]^{\psi=id}$. Now we can formulate the following result.

Proposition 6.2. *The map*

$$[Col] : \mathcal{U}^1_\infty \to \mathbb{Z}_p[[T]]^{\psi=id}$$

is an isomorphism of $\mathbb{Z}_p[[\Gamma]]$-modules. The Coates-Wiles homomorphisms

$$CW_k : \mathcal{U}^1_\infty \to \mathbb{Z}_p(k)$$

are morphisms of $\mathbb{Z}_p[[\Gamma]]$-modules.

Proof. The first part was already shown. The morphisms CW_k are morphisms of $\mathbb{Z}[\Gamma]$-modules, hence they are morphisms of $\mathbb{Z}_p[[\Gamma]]$-modules, as both $\mathcal{U}^1_\infty$ and $\mathbb{Z}_p(k)$ are $\mathbb{Z}_p[[\Gamma]]$-modules. □

We denote by E_n and C_n, the group of units and cyclotomic units, respectively, in $\mathbb{Q}(\mu_{p^n})$. We recall that $\mathbb{Q}(\mu_{p^n})^+$ is the maximal real subfield of $\mathbb{Q}(\mu_{p^n})$. We denote by E^+_n and C^+_n the group of units and cyclotomic units in $\mathbb{Q}(\mu_{p^n})^+$ and by $\mathcal{E}^+_n$ and $\mathcal{C}^+_n$ the group of p-units and cyclotomic p-units in $\mathbb{Q}(\mu_{p^n})^+$.

Lemma 6.3. *The inclusions $E_n \hookrightarrow \mathcal{E}_n$ and $E^+_n \hookrightarrow \mathcal{E}^+_n$ induce isomorphisms*

$$E_n/C_n \xrightarrow{\cong} \mathcal{E}_n/\mathcal{C}_n \ \text{ and } \ E^+_n/C^+_n \xrightarrow{\cong} \mathcal{E}^+_n/\mathcal{C}^+_n.$$

Proposition 6.4. *Let us assume that p does not divide the class number $h(\mathbb{Q}(\mu_p)^+)$, i.e. that the Vandiver conjecture holds for a prime p. Then p does not divide $| \mathcal{E}_n/\mathcal{C}_n |$ for all $n \geqslant 1$.*

Proof. The Vandiver conjecture for p implies that p does not divide the class number $h(\mathbb{Q}(\mu_{p^n})^+)$ for all $n \geqslant 1$ ([14, Corollary 10.6]). Hence p does not divide $|E_n^+/C_n^+|$ for all $n \geqslant 1$ ([14, Theorem 8.2]). We have $E_n = \mu_{p^n} E_n^+$ ([14, Theorem 4.12 and Corollary 4.13]) and $C_n = \mu_{p^n} C_n^+$ ([14, Lemma 8.1]). Hence it follows that $E_n^+/C_n^+ \cong E_n/C_n$. Therefore it follows from the above lemma that p does not divide the order of $\mathcal{E}_n/\mathcal{C}_n$ for all $n \geqslant 1$. □

Let $\mathcal{M}_p$ be the maximal abelian pro-p extension of $\mathbb{Q}(\mu_{p^\infty})$ unramified outside p and let $\mathcal{L}_p$ be the maximal extension of $\mathbb{Q}(\mu_{p^\infty})$ contained in $\mathcal{M}_p$ that is unramified. Local class field theory defines a canonical map of $\mathbb{Z}_p[[\Gamma]]$-modules

$$[CL] : \mathcal{U}_\infty^1 \to Gal(\mathcal{M}_p/\mathbb{Q}(\mu_{p^\infty})).$$

The map $[CL]$ induces a surjective morphism of $\mathbb{Z}_p[[\Gamma]]$-modules

$$[CL] : \mathcal{U}_\infty^1 \to Gal(\mathcal{M}_p/\mathcal{L}_p).$$

The field $\mathcal{K}_p$ is an abelian pro-p extension of $\mathbb{Q}(\mu_{p^\infty})$ unramified outside p. Therefore $\mathcal{K}_p \subset \mathcal{M}_p$. Let $\mathcal{K}_p^0$ be the maximal unramified extension of $\mathbb{Q}(\mu_{p^\infty})$ contained in $\mathcal{K}_p$. We denote the composition of the map $[CL]$ with the natural map

$$Gal(\mathcal{M}_p/\mathbb{Q}(\mu_{p^\infty})) \to Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))$$

by $[cl]$. The image of $[cl]$ is the subgroup $Gal(\mathcal{K}_p/\mathcal{K}_p^0)$ of $Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))$.

The next result we need, is stated without proof in [8, on page 248].

Lemma 6.5. *Let us assume that p does not divide the class number $h(\mathbb{Q}(\mu_p)^+)$,i.e. that the Vandiver conjecture holds for a prime p. Then $\mathcal{K}_p = \mathcal{M}_p^-$.*

Proof. It follows from Proposition 3.1,ii) that $\mathcal{K}_p \subset \mathcal{M}_p^-$. Another proof is in [8, on page 248]. First we shall show that $\mathcal{M}_p^-$ is generated over $\mathbb{Q}(\mu_{p^\infty})$ by p^nth roots of p-units of $\mathbb{Q}(\mu_{p^\infty})^+$ for $n \in \mathbb{N}$.

The extension $\mathbb{Q}(\mu_{p^\infty}) \hookrightarrow \mathcal{M}_p^-$ is pro-p, abelian. Hence it is generated by Kummer extensions of the form $\mathbb{Q}(\mu_{p^n}) \hookrightarrow M = \mathbb{Q}(\mu_{p^n})(a^{1/p^r})$ for some $a \in \mathbb{Z}[\mu_{p^n}]$. We can assume that $a \in \mathbb{Z}[\mu_{p^n}]^+$.

Let $\mathfrak{q}$ be a prime ideal of $\mathbb{Z}[\mu_{p^n}]^+$ not dividing p. If $a \notin \mathfrak{q}$ then the extension $\mathbb{Q}(\mu_{p^n}) \hookrightarrow M$ is unramified over $\mathfrak{q}$. Let us assume that $a \in \mathfrak{q}$. Then the extension M of $\mathbb{Q}(\mu_{p^n})$ is unramified over $\mathfrak{q}$ if and only if $a \in \mathfrak{q}^{kp^r}$ for some $k > 0$ and $a \notin \mathfrak{q}^{kp^r+1}$. If $\mathfrak{q}$ is a principal ideal generated by $q \in \mathbb{Z}[\mu_{p^n}]^+$ then $a = q^{kp^r} a_1$, $a_1 \notin \mathfrak{q}$ and $M = \mathbb{Q}(\mu_{p^n})(a_1^{1/p^r})$. So let us assume that $\mathfrak{q}$ is not a principal ideal. The fact that p does not divide $h(\mathbb{Q}(\mu_p)^+)$ implies that p does not divide $h(\mathbb{Q}(\mu_{p^n})^+)$ (see [14, Corollary 10.6]). Hence there is a positive integer s coprime to p such that $\mathfrak{q}^s$ is a principal ideal generated by some $q \in \mathbb{Z}[\mu_{p^n}]^+$. Observe that $a^s = q^{kp^r} a_1$, $a_1 \notin \mathfrak{q}$ and $\mathbb{Q}(\mu_{p^n})(a_1^{1/p^r}) = M$ by the Kummer theory. Therefore $\mathcal{M}_p^-$ is generated over $\mathbb{Q}(\mu_{p^\infty})$ by p-units of $\mathbb{Q}(\mu_{p^n})^+$ for $n \in \mathbb{N}$.

It follows form [14, Corollary 10.6 and Theorem 8.2] and from Lemma 6.3 that p does not divide $|\ \mathcal{E}_n^+/C_n^+\ |$. Hence it follows from the Kummer theory that $\mathcal{M}_p^-$ is generated over $\mathbb{Q}(\mu_{p^\infty})$ by cyclotomic p-units of $\mathbb{Q}(\mu_{p^n})^+$ for $n \in \mathbb{N}$. The elements $1 - \xi_{p^n}^i$ for i between 0 and $p^n/2$ and coprime to p and ξ_{p^n} generate p-units of $\mathbb{Q}(\mu_{p^n})$. The p-units of $\mathbb{Q}(\mu_{p^n})^+$ can be expressed by these p-units of $\mathbb{Q}(\mu_{p^n})$. Hence it follows that $\mathcal{M}_p^- \subset \mathcal{K}_p$. □

7. The main formula

We recall the formula from [7, page 105]

$$\int_{\mathbb{Z}_p^\times} x^{m-1} d\mathfrak{N}(\overrightarrow{10})([cl](\epsilon))(x) = (p^{m-1}-1)L_p(m,\omega^{1-m})CW_m^\epsilon, \tag{9}$$

for all odd integers $m > 1$ and all $\epsilon \in \mathcal{U}_\infty^1$.

We shall rewrite the formula in terms of integrals over $\mathbb{Z}_p^\times$. It follows from Corollary 5.5 that

$$(1-p^{m-1})CW_m^\epsilon = \int_{\mathbb{Z}_p^\times} x^{m-1} d\mu_{\Delta(f_\epsilon)}^\times(x) \tag{10}$$

for $m \geqslant 1$.

Let $c \in \mathbb{Z}_p^\times - \mu_{p-1}$. We recall that

$$L_p(1-s,\omega^\beta) := \frac{1}{\omega^\beta(c)\langle c\rangle^s - 1} \int_{\mathbb{Z}_p^\times} \langle x\rangle^s x^{-1}\omega^\beta(x) dE_{1,c}^\times(x)$$

by definition (see [10, Chapter 4]).

Let $j : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ be defined by $j(x) = x^{-1}$. Then j induces $j_* : \mathbb{Z}_p[[\mathbb{Z}_p^\times]] \to \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. Let us set

$$\mathcal{E}_c := j_*(E_{1,c}^\times).$$

Finally we define a measure $\mathcal{F}_c$ on $\mathbb{Z}_p^\times$ by

$$d\mathcal{F}_c(x) := x d\mathcal{E}_c(x).$$

It follows from the definition of the measure $\mathcal{F}_c$ that

$$-L_p(m,\omega^{1-m}) = \frac{1}{1-c^{1-m}} \int_{\mathbb{Z}_p^\times} x^{-m} dE_{1,c}^\times(x) = \frac{1}{1-c^{1-m}} \int_{\mathbb{Z}_p^\times} x^{m-1} d\mathcal{F}_c(x) \tag{11}$$

for $m \neq 1$.

Let $c \in \mathbb{Z}_p^\times$. Let δ_c be a measure on $\mathbb{Z}_p^\times$ defined by $\int_{\mathbb{Z}_p^\times} f(x) d\delta_c(x) = f(c)$ for any continuous function f on $\mathbb{Z}_p^\times$. Observe that

$$1 - c^{1-m} = \int_{\mathbb{Z}_p^\times} x^{m-1} d(\delta_1 - \delta_{c^{-1}})(x). \tag{12}$$

Lemma 7.1. *Let $m \geqslant 1$ and let $\epsilon \in \mathcal{U}_\infty^1$. Then*

$$\int_{\mathbb{Z}_p^\times} x^{m-1} d(\delta_1 - \delta_{c^{-1}})(x) \cdot \int_{\mathbb{Z}_p^\times} x^{m-1} d\mathfrak{N}(\overrightarrow{10})^\times([cl](\epsilon))(x) \tag{13}$$

$$= \int_{\mathbb{Z}_p^\times} x^{m-1} d\mathcal{F}_c(x) \cdot \int_{\mathbb{Z}_p^\times} x^{m-1} d\mu_{\Delta(f_\epsilon)}^\times(x)\,.$$

Proof. It follows from (10), (11) and (12) that the formula (9) can be written in the form (13) for $m > 1$ and odd. Observe that the formula (13) holds also for $m = 1$ as then both sides vanish. Notice that the left hand side of the formula (13) vanishes for $m > 0$ and even. On the other side $L_p(m,\omega^{1-m}) = 0$ for m even as then $1 - m$ is odd. Hence equation (11)

implies that the right hand side also vanishes for $m > 0$ and m even. □

Proposition 7.2. *Let $\epsilon \in \mathcal{U}_\infty^1$ and let $c \in \mathbb{Z}_p^\times - \mu_{p-1}$. Then*

$$(\delta_1 - \delta_{c^{-1}}) \cdot (\mathfrak{U}(\overrightarrow{10})^\times([cl](\epsilon))) = \mathcal{F}_c \cdot \mu_{\Delta(f_\epsilon)}^\times \tag{14}$$

in $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$.

Proof. The proposition follows immediately from Lemma 7.1 and Lemma 4.1. □

Let S be the set of all non-zero divisors in the ring $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. We set

$$\mathfrak{F} := S^{-1}\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$$

for the total ring of fractions.

Corollary 7.3. *Let $c \in \mathbb{Z}_p^\times - \mu_{p-1}$ and let $\epsilon \in \mathcal{U}_\infty^1$. Then $[cl](\epsilon) = 0$ in $Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))$ if and only if $(\delta_1 - \delta_{c^{-1}})^{-1} \cdot \mathcal{F}_c \cdot \mu_{\Delta(f_\epsilon)}^\times = 0$ in $\mathfrak{F}$.*

Proof. Following [1, Lemma 4.2.2] the element $\delta_1 - \delta_{c^{-1}}$ is not a zero divisor in $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. Hence

$$\mathfrak{U}(\overrightarrow{10})^\times([cl](\epsilon)) = (\delta_1 - \delta_{c^{-1}})^{-1} \cdot \mathcal{F}_c \cdot \mu_{\Delta(f_\epsilon)}^\times$$

in $\mathfrak{F}$ by Proposition 7.2. The corollary follows from the fact that the map

$$z_p : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty})) \to \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$$

is injective by Proposition 3.1 (i). □

Lemma 7.4. *Let $c, c_1 \in \mathbb{Z}_p^\times - \mu_{p-1}$. Then*

$$(\delta_1 - \delta_{c^{-1}})^{-1} \cdot \mathcal{F}_c = (\delta_1 - \delta_{c_1^{-1}})^{-1} \cdot \mathcal{F}_{c_1}$$

in the ring $\mathfrak{F}$.

Proof. It follows from the formula (11) that

$$(1 - c_1^{1-m}) \int_{\mathbb{Z}_p^\times} x^{m-1} d\mathcal{F}_c(x) = (1 - c^{1-m}) \int_{\mathbb{Z}_p^\times} x^{m-1} d\mathcal{F}_{c_1}(x) \tag{15}$$

for $m > 1$. For $m = 1$ both sides of the equality (15) vanish. Hence it follows from Lemma 4.1 that

$$(\delta_1 - \delta_{c_1^{-1}})\mathcal{F}_c = (\delta_1 - \delta_{c^{-1}})\mathcal{F}_{c_1}$$

in $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. Therefore the lemma follows as $\delta_1 - \delta_{c_1^{-1}}$ and $\delta_1 - \delta_{c^{-1}}$ are not zero divisors in $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. □

Let $f \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. We denote by (f) an ideal of $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ generated by f.

Lemma 7.5. *Let $c \in \mathbb{Z}_p^\times - \mu_{p-1}$. Then $\mathcal{F}_c \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]^-$ and $(\mathcal{F}_c) \subset \mathbb{Z}_p[[\mathbb{Z}_p^\times]]^-$.*

Proof. Observe that $L_p(m, \omega^{1-m}) = 0$ if m is even as then $1 - m$ is odd. Hence it follows from the formula (11) that

$$\int_{\mathbb{Z}_p^\times} x^{m-1} d\mathcal{F}_c(x) = -(1-c^{1-m})L_p(m,\omega^{1-m}) = 0$$

for m even. Hence it follows that $\Phi(\mathcal{F}_c) \in (\prod_{k=1}^{\infty} \mathbb{Z}_p(k))^-$. Therefore it follows from Lemma 4.1 that $\mathcal{F}_c \in \mathbb{Z}_p[[Z_p^\times]]^-$ and also that the ideal $(\mathcal{F}_c) \subset \mathbb{Z}_p[[Z_p^\times]]^-$. □

The augmentation ideal of $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ is the ideal

$$I(\mathbb{Z}_p^\times) := \{\nu \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]] : \int_{\mathbb{Z}_p^\times} d\nu(x) = 0\}.$$

DEFINITION 7.6. Let $c \in \mathbb{Z}_p^\times - \mu_{p-1}$. We define an element ζ_p in $\mathfrak{F}$ by

$$\zeta_p := -(\delta_1 - \delta_{c^{-1}})^{-1} \cdot \mathcal{F}_c\,.$$

It follows from Lemma 7.4 that the element $\zeta_p \in \mathfrak{F}$ does not depend on a choice of $c \in \mathbb{Z}_p - \mu_{p-1}$. Moreover it follows from [1, Lemma 4.2.4] that ζ_p is a pseudo-measure.

We recall that the ring $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ is a subring of $\mathfrak{F}$. The set $I(\mathbb{Z}_p^\times)\zeta_p$ is a subset of $\mathfrak{F}$. We shall show that it is in fact an ideal of the ring $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$.

Lemma 7.7. *Let $c \in \mathbb{Z}_p^\times - \mu_{p-1}$ be such that its class modulo p^2 generates $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Then*

$$(\mathcal{F}_c) = I(\mathbb{Z}_p^\times)\zeta_p\,,$$

hence $I(\mathbb{Z}_p^\times)\zeta_p$ is an ideal of $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$.

The standard proof, which however require the use of [1, Lemma 4.2.5], we omit.

DEFINITION 7.8. We define an ideal (ζ_p) of $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ to be the ideal $I(\mathbb{Z}_p^\times)\zeta_p$ of $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$.

Proposition 7.9. *Let $\tilde{\zeta}_p$ be a pseudo-measure on $\mathbb{Z}_p^\times$ considered in* [1, Proposition 4.2.4]. *Then the relation between ζ_p defined in this paper and $\tilde{\zeta}_p$ is given by $j_*(\zeta_p) = -\tilde{\zeta}_p$.*

Proof. We recall that

$$\int_{\mathbb{Z}_p^\times} x^k d\tilde{\zeta}_p(x) = -(1-p^{k-1})\frac{B_k}{k}$$

for $k = 1, 2, 3\ldots$ (see [1, Proposition 4.2.4]). On the other side

$$\frac{1}{1-c^k}\int_{\mathbb{Z}_p^\times} x^k \cdot x^{-1} dE_{1,c}^\times(x) = (1-p^{k-1})\frac{B_k}{k}$$

for $k = 1, 2, 3\ldots$ by [10, Chapter 2, Theorem 2.3 and Chapter 10, Theorem 2.1]. Hence it follows that

$$-(\delta_1 - \delta_c)^{-1} x^{-1} dE_{1,c}^\times(x) = d\tilde{\zeta}_p(x)\,.$$

Applying j_* to the left hand side we get that

$$-(\delta_1 - \delta_{c^{-1}})^{-1} x d(j_*(E_{1,c}^\times))(x) = -(\delta_1 - \delta_{c^{-1}})^{-1} d\mathcal{F}_c(x)\,.$$

Hence it follows that $j_*(\zeta_p) = -\tilde{\zeta}_p$ in $\mathfrak{F}$. □

8. Proof of the main conjecture assuming the Vandiver conjecture

Let

$$C : \mathcal{U}_\infty^1 \to \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$$

be a map defined by $C(\epsilon) := \mu^\times_{\Delta(f_\epsilon)}$.

Lemma 8.1. *The image of the map $C : \mathcal{U}_\infty^1 \to \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ is equal to $I(\mathbb{Z}_p^\times)$.*

Proof. It follows from Proposition 6.2 that the image of $\mathcal{U}_\infty^1$ by the map $[Col]$ is equal to $\mathbb{Z}_p[[T]]^{\psi=id}$. Let $f \in \mathbb{Z}_p[[T]]^{\psi=id}$. Then it follows from Corollary 5.4 that

$$\mathcal{P}(\mu_f^\times)(0) = \int_{\mathbb{Z}_p^\times} d\mu_f^\times = 0\,.$$

Hence it follows that $\mu^\times_{\Delta(f_\epsilon)} \in I(\mathbb{Z}_p^\times)$ for $\epsilon \in \mathcal{U}_\infty^1$.

Let $\nu \in I(\mathbb{Z}_p^\times)$. Then $\mathcal{P}(\nu) \in \mathbb{Z}_p[[T]]^{\psi=0}$ and $\mathcal{P}(\nu)(0) = 0$ by [1, Lemma 3.4.1]. It follows from [1, Lemma 2.4.3] that there is $g \in \mathbb{Z}_p[[T]]^{\psi=id}$ such that $\mathcal{P}(\nu) = g - \varphi(g)$. Moreover $g = [Col](\epsilon) = \Delta(f_\epsilon)$ for some $\epsilon \in \mathcal{U}_\infty^1$ by Proposition 6.2. We have

$$\mathcal{P}(\mu^\times_{\Delta(f_\epsilon)}) = \Delta(f_\epsilon) - \phi(\Delta(f_\epsilon)) = g - \phi(g) = \mathcal{P}(\nu)$$

by Lemma 5.3. Hence it follows that $\nu = \mu^\times_{\Delta(f_\epsilon)}$. □

We recall that $\mathcal{K}_p^0$ is the maximal unramified extension of $\mathbb{Q}(\mu_{p^\infty})$ contained in $\mathcal{K}_p$.

Proposition 8.2. *The map*

$$Gal(\mathcal{K}_p/\mathcal{K}_p^0) \to (\zeta_p)$$

given by $\sigma \mapsto \mathfrak{A}(\overrightarrow{10})^\times(\sigma)$ is an isomorphism of $\mathbb{Z}_p[[\Gamma]]$-modules.

Proof. Following Proposition 3.1 the morphism

$$z_p^- : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty})) \to \mathbb{Z}_p[[\mathbb{Z}_p^\times]]^-$$

is an injective morphism of $\mathbb{Z}_p[[\Gamma]]$-modules. Let $c \in \mathbb{Z}_p^\times - \mu_{p-1}$ be such that its class modulo p^2 generates $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Following [1, Lemma 4.2.5]

$$I(\mathbb{Z}_p^\times) = (\delta_1 - \delta_{c^{-1}})\mathbb{Z}_p[[\mathbb{Z}_p^\times]]\,.$$

Hence it follows that

$$(\delta_1 - \delta_{c^{-1}})^{-1} I(\mathbb{Z}_p^\times) = \mathbb{Z}_p[[\mathbb{Z}_p^\times]]\,. \tag{16}$$

The image of the map

$$[cl] : \mathcal{U}_\infty^1 \to Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty}))$$

is equal to $Gal(\mathcal{K}_p/\mathcal{K}_p^0)$. Hence it follows from Proposition 7.2, Lemma 8.1 and the equality (16) that

$$z_p^-(Gal(\mathcal{K}_p/\mathcal{K}_p^0)) = (\zeta_p)\,.$$

□

We recall from Introduction that $\mathcal{L}_p$ is the maximal abelian pro-p, contained in $\mathcal{M}_p$, extension of $\mathbb{Q}(\mu_{p^\infty})$ unramified everywhere. Now we shall prove the main conjecture assuming the Vandiver conjecture for a prime p.

Proposition 8.3. *Let us assume that p does not divide the class number $h(\mathbb{Q}(\mu_p)^+)$,i.e. that the Vandiver conjecture holds for a prime p. Then we have an isomorphism of $\mathbb{Z}_p[[\Gamma]]$-modules*

$$Gal(\mathcal{L}_p^-/\mathbb{Q}(\mu_{p^\infty})) \cong \mathbb{Z}_p[[\mathbb{Z}_p^\times]]^-/(\zeta_p)\,.$$

Proof. We recall that (ζ_p) is an ideal of $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ and it is contained in $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]^-$. It follows from Lemma 6.5 that $\mathcal{M}_p^- = \mathcal{K}_p$. Therefore $\mathcal{L}_p^- = \mathcal{K}_p^0$. The morphism

$$z_p^- : Gal(\mathcal{K}_p/\mathbb{Q}(\mu_{p^\infty})) \to \mathbb{Z}_p[[\mathbb{Z}_p^\times]]^-$$

is an isomorphism of $\mathbb{Z}_p[[\Gamma]]$-modules by Proposition 6.4 and by Lemma 3.3. Hence it follows from Proposition 8.2 that $Gal(\mathcal{K}_p^0/\mathbb{Q}(\mu_{p^\infty})) \cong \mathbb{Z}_p[[\mathbb{Z}_p^\times]]^-/(\zeta_p)$ □

9. The Ihara formula for all *m*

In this section we show that the Ihara formula from Introduction holds for all m. In fact only the case $m = 1$ requires a careful proof.

Lemma 9.1. *Let $c \in \mathbb{Z}_p^\times - \mu_{p-1}$. Then*

$$\int_{\mathbb{Z}_p^\times} d\mathcal{F}_c(x) = (1 - p^{-1}) \log(c^{-1}).$$

Proof. We recall that $E_{1,c}$ is the regularized Bernoulli measure and $E_{1,c}^\times$ is its restriction to $\mathbb{Z}_p^\times$. The power series $\mathcal{P}(E_{1,c})$ is equal $1/T - c/((1+T)^c - 1)$ (see [10, Chapter 4, Proposition 3.4]). Hence it follows from [1, Lemma 3.4.1] and the formula at the end of the proof of Lemma 2.6 in [12] that

$$\mathcal{P}(E_{1,c}^\times)(T) = \frac{1}{T} - \frac{c}{(1+T)^c - 1} - \frac{1}{(1+T)^p - 1} + \frac{c}{(1+T)^{pc} - 1}\,.$$

Observe that $\varepsilon = \left(\frac{\xi_{p^{n+1}} - 1}{\xi_{p^{n+1}}^c - 1}\right)_{n\in\mathbb{N}} \in \mathcal{U}_\infty$. The corresponding power series $f_\varepsilon = \frac{T}{(1+T)^c - 1}$ belongs to W. Let us set

$$g(T) := \log\Big(\frac{T}{(1+T)^c - 1}\Big) - \frac{1}{p}\log\Big(\frac{(1+T)^p - 1}{(1+T)^{pc} - 1}\Big).$$

It follows from [1, Lemma 2.5.1] that $g(T) \in \mathbb{Z}_p[[T]]^{\Psi=0}$. The operator D defined by $(Df)(T) := (1+T)f'(T)$ is an automorphism of $\mathbb{Z}_p[[T]]^{\Psi=0}$ (see [3, Corollary on page 2]). One checks that

$$Dg = \mathcal{P}(E_{1,c}^\times)\,.$$

Therefore

$$\int_{\mathbb{Z}_p^\times} d\mathcal{F}_c(x) = \int_{\mathbb{Z}_p^\times} x^{-1} dE_{1,c}^\times(x) = (D^{-1}\mathcal{P}(E_{1,c}^\times))(0) = g(0) = (1 - p^{-1})\log(c^{-1})$$

(see [12, Lemma 3.4]). □

We define a sequence of $\mathbb{Z}_p$-algebra isomorphisms:

$$\mathbb{Z}_p[[\mathbb{Z}_p^\times]] \to \mathbb{Z}_p[[\mu_{p-1} \times (1 + p\mathbb{Z}_p)]]\,,$$

$$\mathbb{Z}_p^\times \ni [x] \mapsto [\omega(x), x\omega(x)^{-1}] \in \mathbb{Z}_p[[\mu_{p-1} \times (1 + p\mathbb{Z}_p)]];$$

$$\mathbb{Z}_p[[\mu_{p-1} \times (1 + \mathbb{Z}_p)]] \to \mathbb{Z}_p[\Delta][[1 + p\mathbb{Z}_p]],\ [\varepsilon, x] \mapsto \varepsilon[x],$$

where we view μ_{p-1} as an abstract group denoted by Δ;

$$\mathbb{Z}_p[\Delta][[1 + p\mathbb{Z}_p]] \to \mathbb{Z}_p[\Delta][[\mathbb{Z}_p]],\ [x] \mapsto [\frac{\log x}{\log q}],$$

where $q = p + 1$ if $p \neq 2$ and $q = 5$ if $p = 2$. The composition of these isomorphisms we denote by α. Let

$$\varepsilon : \mathbb{Z}_p[\Delta][[\mathbb{Z}_p]] \to \mathbb{Z}_p[[\mathbb{Z}_p]]$$

be the augmentation map with respect to Δ. Let us set

$$A := \varepsilon \circ \alpha\,.$$

Then A is also a morphism of $\mathbb{Z}_p$-algebras.

Lemma 9.2. *Let $\mu \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. Then*

$$\int_{\mathbb{Z}_p^\times} d\mu = \int_{\mathbb{Z}_p} dA(\mu)\,.$$

Proof. One cheks that the formula is true for any $\mu \in \mathbb{Z}_p[\mathbb{Z}_p^\times]$. Hence by continuity the formula holds for any $\mu \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. □

Lemma 9.3. *Let $\mu \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ be such that $\int_{\mathbb{Z}_p^\times} d\mu = 0$. Let $c \in \mathbb{Z}_p^\times$ be such that its class modulo p^2 generates $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Then there exists a unique $\nu \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ such that*

$$\mu = (\delta_1 - \delta_c) \cdot \nu$$

and

$$\int_{\mathbb{Z}_p^\times} d\nu = \Big(-\frac{\log q}{\log c}\Big) \int_{\mathbb{Z}_p} x dA(\mu)(x)\,.$$

Proof. It follows from [1, Lemma 4.2.5] and from the fact that $\delta_1 - \delta_c$ is not a zero divisor (see [1, proof of Lemma 4.2.2]) that there is a unique $\nu \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ such that

$$\mu = (\delta_1 - \delta_c) \cdot \nu$$

in $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. Applying the $\mathbb{Z}_p$-algebra homomorphism A to the above formula we get

$$A(\mu) = (\delta_0 - \delta_{x_0}) \cdot A(\nu)$$

in $\mathbb{Z}_p[[\mathbb{Z}_p]]$, where $x_0 = \frac{\log c}{\log q}$. Hence we have the following equality of power series in $\mathbb{Z}_p[[T]]$

$$\mathcal{P}(A(\mu))(T) = (1 - (1 + T)^{x_0}) \cdot \mathcal{P}(A(\nu))(T)\,.$$

It follows from Lemma 9.2 that

$$\mathcal{P}(A(\mu))(0) = \int_{\mathbb{Z}_p} dA(\mu) = \int_{\mathbb{Z}_p^\times} d\mu = 0\,.$$

Comparing the coefficients at T we get

$$\int_{\mathbb{Z}_p} xdA(\mu)(x) = (-x_0)\int_{\mathbb{Z}_p} dA(\nu) = (-x_0)\int_{\mathbb{Z}_p^\times} d\nu\,.$$

□

In the next proposition we present the analogue of the Ihara formula from Introduction for $m = 1$. Notice that $1 - p^{-1}$ appearing in our formula is the residue of the p-adic zeta function of Kubota-Leopoldt.

Proposition 9.4. *Let $\epsilon \in \mathcal{U}_\infty^1$. Then we have*

$$\kappa(p)([cl](\epsilon)) = \int_{\mathbb{Z}_p^\times} d\mathfrak{U}(\overrightarrow{10})([cl](\epsilon)) = (1-p^{-1})(-\log q \int_{\mathbb{Z}_p} xdA(\mu^\times_{\Delta(f_\epsilon)})(x))\,.$$

Proof. Let $c \in \mathbb{Z}_p^\times$ be such that its class modulo p^2 generates $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Following Corollary 5.4 $\int_{\mathbb{Z}_p^\times} d\mu^\times_{\Delta(f_\epsilon)} = 0$. Hence it follows from Lemma 9.3 that there is a unique $\nu_{\epsilon,c} \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ such that

$$\mu^\times_{\Delta(f_\epsilon)} = (\delta_1 - \delta_{c^{-1}})\cdot \nu_{\epsilon,c}\,.$$

Hence it follows from Proposition 7.2 that

$$\mathfrak{U}(\overrightarrow{10})^\times([cl](\epsilon)) = \mathcal{F}_c \cdot \nu_{\epsilon,c}\,.$$

It follows from Lemma 4.1 that

$$\int_{\mathbb{Z}_p^\times} d\mathfrak{U}(\overrightarrow{10})^\times([cl](\epsilon)) = \int_{\mathbb{Z}_p^\times} d\mathcal{F}_c \cdot \int_{\mathbb{Z}_p^\times} d\nu_{\epsilon,c}\,.$$

Let us observe that $\int_{\mathbb{Z}_p^\times} d\mathfrak{U}(\overrightarrow{10})(\sigma)^\times = \kappa(p)(\sigma)$ for any $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$. On the other side

$$\begin{aligned}\int_{\mathbb{Z}_p^\times} d\mathcal{F}_c \cdot \int_{\mathbb{Z}_p^\times} d\nu_{\epsilon,c} &= (1-p^{-1})\log(c^{-1})\Big(-\frac{\log q}{\log(c^{-1})}\int_{\mathbb{Z}_p} xdA(\mu^\times_{\Delta(f_\epsilon)})(x)\Big)\\ &= (1-p^{-1})(-\log q\int_{\mathbb{Z}_p} xdA(\mu^\times_{\Delta(f_\epsilon)})(x))\end{aligned}$$

by Lemmas 9.1 and 9.3. □

Let us define

$$\Psi : \mathbb{Z}_p[[\mathbb{Z}_p^\times]] \to \prod_{k=-\infty}^{\infty} \mathbb{Z}_p(k)$$

by the formula

$$\Psi(\mu) = \Big(\int_{\mathbb{Z}_p^\times} x^{k-1} d\mu(x)\Big)_{k=-\infty}^{\infty}\,.$$

As in the proof of Lemma 4.1 one checks that $\Psi(\mu\cdot\nu) = \Psi(\mu)\Psi(\nu)$. Hence it follows from

Proposition 7.2 that

$$(1-c^{1-k})\Big(\int_{\mathbb{Z}_p^\times} x^{k-1}d\mathfrak{A}(\overrightarrow{10})^\times([cl](\epsilon))\Big) = \Big(\int_{\mathbb{Z}_p^\times} x^{k-1}d\mathcal{F}_c(x)\Big)\Big(\int_{\mathbb{Z}_p^\times} x^{k-1}d\mu^\times_{\Delta(f_\epsilon)}(x)\Big)\,.$$

Following (11), $\int_{\mathbb{Z}_p^\times} x^{k-1}d\mathcal{F}_c(x) = -(1-c^{1-k})L_p(k,\omega^{1-k})$ for $k \neq 1$. Hence we have proved the following result.

Proposition 9.5. *Let $\epsilon \in \mathcal{U}^1_\infty$. For $k \neq 1$ we have*

$$\int_{\mathbb{Z}_p^\times} x^{k-1}d\mathfrak{A}(\overrightarrow{10})^\times([cl](\epsilon)) = -L_p(k,\omega^{1-k})\int_{\mathbb{Z}_p^\times} x^{k-1}d\mu^\times_{\Delta(f_\epsilon)}(x)\,.$$

Remark 9.6. If $k = 1$ then in the formula of Proposiotion 9.5 the left hand side is equal to $\kappa(p)([cl](\epsilon))$. On the right hand side of the formula, $\int_{\mathbb{Z}_p^\times} d\mu^\times_{\Delta(f_\epsilon)}(x) = 0$ by Corollary 5.4, while $L_p(1,\omega^0)$ is not defined if we use the definition of the function $L_p(1-s,\omega^\beta)$ given at the beginning of Section 7. The integral $\int_{\mathbb{Z}_p^\times}\langle x\rangle^s x^{-1}\omega^\beta(x)dE^\times_{1,c}(x)$ is well defined for $s = 0$ and $\beta = 0$ but the function $s \mapsto \frac{1}{\langle c\rangle^s - 1}$ has a pole at $s = 0$.

Acknowledgements. The second author would like to thank very much Hiroaki Nakamura for discussions.

References

[1] J. Coates and R. Sujatha: Cyclotomic fields and zeta values, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2006.

[2] R. Coleman: *Anderson-Ihara theory: Gauss sums and circular units*; in Algebraic number theory, Adv. Stud. Pure Math. **17**, Academic Press, Boston, MA, 1989, 55–72.

[3] R. Coleman: *Local units modulo circular units*, Proc. Amer. Math. Soc. **89** (1983), 1–7.

[4] I.B. Fesenko and S.V. Vostokov: Local fields and their extensions, Translations of Mathematical Monographs **121**, second ed., American Mathematical Society, Providence, RI, 2002.

[5] H. Ichimura and M. Kaneko: *On the Universal Power Series for Jacobi Sums and the Vandiver Conjecture*, J. Number Theory **31** (1989), 312–334.

[6] H. Ichimura and K. Sakaguchi: *The nonvanishing of a certain Kummer character χ_m (after C. Soulé), and some related topics*: in Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986), Adv. Stud. Pure Math. **12**, North-Holland, Amsterdam, 1987, 53–64.

[7] Y. Ihara: *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. (2), **123** (1986), 43–106.

[8] Y. Ihara: *Some arithmetic aspects of Galois actions in the pro-p fundamental group of P′t*0, 1, 8*u*; in Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math. **70**, Amer. Math. Soc., Providence, Ri, 2002, 247–273.

[9] G. Kings: *On p-adic Interpolation of Motivic Eisenstein Classes*; In Elliptic Curves, Modular Forms and Iwasawa Theory, Springer Proc. Math. Stat. **188**, Springer, Cham, 2016, 335–371.

[10] S. Lang: Cyclotomic fields I and II, combined second ed., Graduate Texts in Mathematics **121**, Springer-Verlag, New York, 1990.

[11] B. Mazur and A. Wiles: *Class field of abelian extensions of* $\mathbb{Q}$, Invent. Math. **76** (1984), 179–330.

[12] H. Nakamura, K. Sakugawa, and Z. Wojtkowiak: *Polylogarithmic analogue of the Coleman-Ihara formula*, I, Osaka J. Math. **54** (2017), 55–74.

[13] H. Nakamura and Z. Wojtkowiak: *On explicit formulae for l-adic polylogarithms*; in Arithmetic fundamen-

tal groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math. **70**, Amer. Math. Soc., Providence, Ri, 2002, 285–294.
[14] L.C. Washington: Introduction to cyclotomic fields, second ed., Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1997.
[15] Z. Wojtkowiak: *On ℓ-adic iterated integrals, I Analog of Zagier Conjecture*, Nagoya Math. J. **176** (2004), 113–158.
[16] Z. Wojtkowiak: *On ℓ-adic Galois L-functions*; in Algebraic geometry and number theory, Progr. Math. **321**, Birkhäuser/Springer, Cham, 2017, 161–209.
[17] Z. Wojtkowiak: *On $\hat{\mathbb{Z}}$-zeta function*; in Iwasawa theory 2012, Contrib. Math. Comput. Sci. **7**, Springer, Heidelberg, 2014, 471–483.

Mahesh Kakde
King's College London
Department of Mathematics
London WC2R 2LS
U.K.
e-mail: mahesh.kakde@kcl.ac.uk

Zdzisław Wojtkowiak
Laboratoire Jean Alexandre Dieudonné
UMR No 7351 CNRS UNS
Départment de Mathématiques
Université de Nice-Sophia Antipolis
Parc Valrose – B.P.No. 71, 06108, Nice Cedex 02
France
e-mail: wojtkow@unice.fr